Chip and PIN is Broken

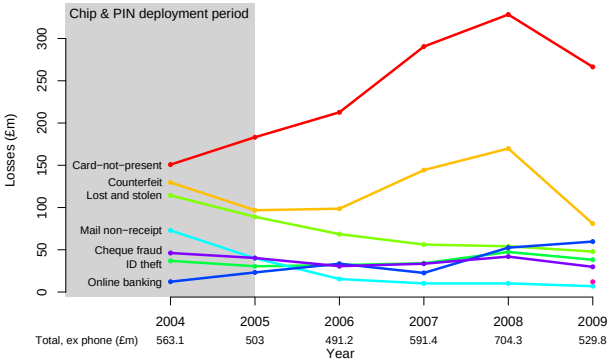
Vulnerabilities in the EMV card payments system

Steven J. Murdoch, Saar Drimer, Ross Anderson, Mike Bond

UNIVERSITY OF CAMBRIDGE
Computer Laboratory
Security Group

Chip and PIN (EMV)

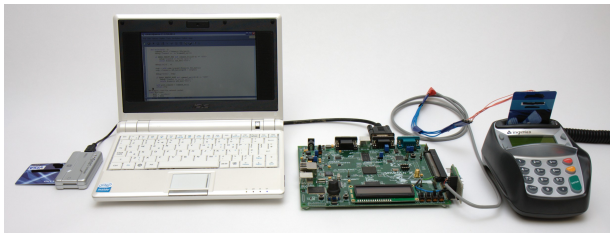
Known in the UK as "Chip and PIN", EMV (Europay, MasterCard, Visa) is the dominant standard for smart-card payments worldwide. Introduced to reduce card fraud, EMV is used throughout Europe; it is being introduced in Canada and South America; and there is pressure to introduce it in the US. EMVCo estimates that over a billion EMV payment cards are in circulation. EMV makes card transactions more secure by adding a chip to cards to make them harder to counterfeit and requiring customers to enter a PIN to authorize payment (hence "Chip and PIN"). While initially reducing fraud, criminals adapted to the change, resulting in increased losses.



Source: UK Cards Association, 2010

The No-PIN vulnerability

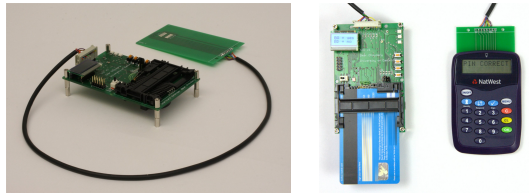
Our paper describes a flaw we discovered in EMV which allows criminals to use stolen cards to make payments without knowing their PIN and remain undetected. To do this, the fraudsters perform what is known as a man-in-the-middle attack, effectively placing themselves between the card and the payment terminal. They then: (1) trick the terminal into believing that the PIN was entered correctly, allowing the transaction to proceed; (2) tell the card that a PIN is not required and to allow the transaction to proceed; and (3) prevent the discrepancy from being uncovered by not allowing the card and the terminal to talk directly to each other. By the time the fraudulent transaction is noticed or the card reported missing, the criminals would have left with the goods; the victim is left out of pocket and may have to challenge bank records for reimbursement.



Initial version of attack demonstration equipment

We demonstrated that this vulnerability could be exploited on the BBC Newsnight TV programme.

BBC Newsnight, BBC 2, 2010-02-11



Miniaturized attack demonstration equipment, designed by Omar Choudary

We notified the banking industry of this flaw in November 2009, yet as of July 2010 the UK Chip and PIN system remains vulnerable. We understand that a defence against the attack is under development but has not yet been deployed due to concerns that it will block legitimate transactions.

Systemic risks

The flaw we identified affects all UK banks, and others overseas. This illustrates rising systemic risks due to more widespread use of advanced technology in global payment systems – risks, both of fraud and third-party liability, which can affect companies and individuals worldwide. The increased complexity that smart-cards bring is raising the probability of a serious system failure; the international standardization of payment cards is increasing the cost of failure. This combination has major impact on the cost and scale of insurance payouts, and must be reflected in pricing.

> *"...although [the Cambridge researchers] have raised a clear secrity concern with regards to Chip and PIN which we are taking very seriously, the problem highlighted is relevant to all card issuers and not just HSBC"*
>
> Statement from HSBC to BBC Newsnight

The risk of a complete EMV failure and when this might occur are hard to predict. Mitigations, too, can be expensive and can undermine consumer confidence and global trade. Some of that cost may be borne directly and indirectly by insurance. However, insurance can also play an important role in managing these risks, e.g. by incentivizing better system-security design rather the focusing on short-term reductions in unsophisticated fraud.

http://www.cl.cam.ac.uk/research/security/banking/ 2010-11-23